

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

INVENTOR: Blake Earl Hayward

CASE: P3953

SERIAL NO.: 09/661,589

GROUP ART UNIT: 2155

FILED: 09/14/2000

EXAMINER: Bruckart, Benjamin R.

SUBJECT: Network-Based Verification and Fraud-Prevention System

PARTY IN INTEREST: All inventions in the disclosure in the present case are
assigned to or assignable to: Yodlee.Com, Inc.

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sirs:

APPEAL BRIEF

1.0 Real Party in Interest

The real party in interest is Yodlee.Com, Inc.

2.0 Related Appeals and Interferences

This is an appeal from the Office Action of the Examiner dated February 19, 2008, finally rejecting claims 29, 31-34 and 36-38.

3.0 Status of the Claims

Following is the status of all claims in the instant case:

- 1 -28. Canceled.
- 29. Rejected - appealed in this brief; independent.
- 31. Rejected - appealed in this brief; dependent.
- 32. Rejected - appealed in this brief; dependent.
- 33. Rejected - appealed in this brief; dependent.
- 34. Rejected - appealed in this brief; independent.
- 35. Canceled.
- 36. Rejected - appealed in this brief; dependent.
- 37. Rejected - appealed in this brief; dependent.
- 38. Rejected - appealed in this brief; dependent.

4.0 Status of Amendments

No amendments have been filed subsequent to the rejection of claims 29, 31-34, 36-38, the subjects of this appeal.

5.0 Summary of the Claimed Subject Matter

Following is a concise explanation of the subject matter defined in the independent claim including its dependent claims.

5.1 Independent system claim 29

29. A system for fraud prevention by authenticating a user at a first Internet site, comprising (Fig. 16, 295; 303):

an Internet-connected verification server for performing the authentication (Fig. 16, 323; 309; pg. 81, lines 3-4); and

an Internet-connected appliance operable by the user for sending a request for authentication to the first Internet site (Fig. 16, 303; 309; pg. 81, lines 19-22)

wherein the user specifies a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user, and the server, in response to the request, causes automatic navigation to the second and third sites and attempts a login on behalf of the user with the username-password pair, successful login at the second and third sites allowing authentication of the user at the first Internet site (pg. 89, lines 16 to pg. 90, line 5; Fig. 19).

Independent claim 29 provides a system for fraud prevention wherein a user requests authentication/verification at a first Internet site, the request including a user name and password pair, and a server performing the authentication, automatically navigates to a second and third Internet site, not associated with the first Internet site, and the server logs in to the second and third Internet sites using the user's name and password pair, successful login at the second and third sites allowing authentication of the user at the first Internet site.

5.2 dependent claims 31-33

31. The system of claim 29 wherein the verification server is a first server, and the request is sent from the appliance to a second server on the Internet which forwards at least a portion of the request to the first server, and the first server returns an indication of verification after causing the navigation and log-in attempt to the second and third sites provided by the user (pg. 86, lines 25-28; pg. 89, lines 16-22).

32. The system of claim 29 wherein all or a portion of the request is compared against stored user profile data for verification purposes (pg. 89, lines 16-25).

33. The system of claim 29 wherein the request comprises at least three or more user specified network destination sites and user-name-password pairs for the sites, and authentication is a number based on log-in results (pg. 90, lines 1-5).

5.3 Independent method claim 34

34. A method for fraud prevention by authenticating a user at a first Internet site (Fig. 16, 295; 303), comprising steps of:

- (a) accepting by a server an authentication request from the user comprising at least a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair for each site and the username-password pairs are included in the authentication request from the user;

- (b) causing, by the server, automatic navigation to the second and third sites and an automatic login attempt on behalf of the user with the username-password pairs; and

- (c) reporting an indication of authenticity of the user according to success or failure of the login attempts (Fig. 19, pg. 89, line 6 to pg. 90, line 14).

Claim 34 provides a method for fraud prevention by authenticating a user at a first Internet site, comprising steps of: accepting by a server an authentication request from a user comprising at least a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair for each site and the username-password pairs are included in the authentication request from the user; as a result of receiving the request the server automatically navigates to the second and third sites, and attempting an automatic login on behalf of the user with the username-password pairs and reporting an indication of authenticity of the user according to success or failure of the login attempts.

5.4 dependent claims 23-28

36. The method of claim 34 wherein the server is a first server, and the request is sent from the appliance to a second server on the network, which forwards at least a portion of the request to the first server, and the first server returns the indication of authenticity after causing the navigation and log-in attempt at the sites provided by the user (pg. 86, lines 25-28; pg. 89, lines 16-22).

37. The method of claim 34 wherein all or a portion of the request is compared against stored user profile data for verification purposes (pg. 89, lines 16-25).

38. The method of claim 34 wherein the request comprises three or more user specified Internet sites and username-password pairs for the sites, and authentication is a number based on log-in results (pg. 90, lines 1-5).

6. Grounds of Rejection to be Reviewed on Appeal

The Examiner finally rejects claims 29, 30-34, 36-38 under 35 U.S.C. 103(a) as being unpatentable by U.S. Patent No. 6,496,855 by Hunt et al., hereinafter Hunt.

7. Argument

Following is a presentation of arguments put forth by the Examiner and responded to by Appellant.

7.1 35 U.S.C. 35 U.S.C. 103(a) against claim 29

The Examiner's Arguments Regarding Independent Claim 29:

Regarding claim 29, the Hunt reference teaches

a system for fraud prevention by authenticating a user at a first Internet site (Hunt: col. 2, lines 47-51 shows a user is verified; col. 4, lines 11-22, 30-41 teach protecting data for preventing fraud), comprising:

an Internet-connected verification server for performing the authentication (Hunt: col. 2, lines 36-51; the server); and

an Internet-connected appliance operable by the user for sending a request for authentication to the first Internet site (Hunt: col. 1, lines 56-61; the user; col. 5, lines 1-10; RAS);

wherein the user specifies sites not associated with the first Internet site known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user (Hunt: col. 2, lines 47-60; col. 6, lines 48-52; Fig. 1), and the server, in response to the request causes automatic navigation to sites and attempts a login on behalf of the user with the username-password pair, successful login at the sites allowing authentication of the user at the first Internet site (Hunt: col. 4, lines 1-5, 23-26).

The Hunt reference does not explicitly state a second and third Internet sites. However, the Hunt reference does address the plurality of Internet sites that a user registers and authenticates with as a problem in which the invention is overcoming (Hunt: col. 1, lines 21-23, 30-35) in order to protect user data and privacy with the

growth number of sites a user registers with (Hunt; col. 1, lines 21-54).

It would have been obvious at the time of the invention to one of ordinary skill in the art to create the system of fraud preventing by Hunt to include a second and third site that a client wishes to login as taught in the background of Hunt in order to protect user data and privacy with the growth number of sites a user registers with (Hunt; col. 1, lines 21-54).

Appellant's Response

Appellant's claim 29 clearly recites a system for fraud prevention by authenticating a user at a first Internet site. The Examiner states Hunt teaches a fraud prevention system, providing (Hunt; col. 2, lines 47-51 shows a user is verified; col. 4, lines 11-22, 30-41 teach protecting data for preventing fraud) to support the statement.

Appellant points out that Hunt is concerned with alleviating the user of having to repeatedly enter username, passwords and form filling at each Web site visited when navigating the Internet and to protect user data (email address) from being abused by the Internet site by giving protected email addresses to sites when a user registers through the system's interface. The site does not receive the user's real address, but is instead given a unique proxy address by the registration processing system 11 (a different one for each site). (col. 4, lines 1-16) Appellant argues that the teachings of Hunt provided by the Examiner fails to read on a fraud prevention system, as claimed. Hunt provides a system to prevent a user from receiving spam in their email and provides easy log-in at a plurality of a user's registered Web sites.

Appellant argues that Hunt teaches:

"Preferably, each of the service computer or server nodes is a website having a server connected to an internet or intranet. Preferably, the at least one registration agent computer or registration agent server node is connected to an internet, intranet or internet protocol (IP) network." (Hunt col. 2, lines 36-40)

Appellant argues the server referenced by the Examiner in said portion of Hunt reproduced above does not perform authentication of users in a fraud prevention system, as claimed. Hunt provides a single interface to Web sites wherein a user logs into said interface and user information is provided to various Web sites the user navigates to. A user profile is stored in the art of Hunt for each user which holds all of the passwords and usernames, registered Web sites, email addresses etc. As the user navigates the system to the registered Web sites the system of Hunt automatically provides the username/password. There is no teaching of the user sending request for authentication to the first Web site, as claimed. Navigating to a user's site and providing log-in information does not qualify as sending a request for authentication, as claimed. The manual entering of username and password is manually logging in, not requesting authentication, as claimed.

Functional limitation

wherein the user specifies a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user, and the server, in response to the request, causes automatic navigation to the second and third sites and attempts a login on behalf of the user with the username-password pair, successful login at the second and third sites allowing authentication of the user at the first Internet site.

The Examiner admits that Hunt fails to teach a second and third Internet site. The Examiner states Hunt teaches; "wherein the user specifies sites not associated with the first Internet site known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user (Hunt: col. 2, lines 47-60; col. 6, lines 48-52; Fig. 1), and the server, in response to the request causes automatic navigation to sites and attempts a login on behalf of the user with the username-password pair, successful login at the sites allowing authentication of the user at the first Internet site (Hunt: col. 4, lines 1-5, 23-26)."

Appellant argues that in addition to failing to teach a second and third Internet site, Hunt also fails to teach a user making a request for authentication including specifies sites not associated with the first Internet site known to the user as capable of accepting the user's username-password pair included in the request for authentication. **Hunt also fails to teach using successful log-in at the second and third sites allowing authentication at the first site. Appellant argues that the Examiner neglects to consider said limitation nor is there an attempt by the Examiner to show it in the art.** Instead, the Examiner states that; "However, the Hunt reference does address the plurality of Internet sites that a user registers and authenticates with as a problem in which the invention is overcoming (Hunt: col. 1, lines 2 1-23, 30-35) in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

It would have been obvious at the time of the invention to one of ordinary skill in the art to create the system of fraud preventing by Hunt to include a second and third site that a client wishes to login as taught in the background of Hunt in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54)."

Appellant argues that even if it were obvious to include a second and third Internet site in Hunt (which Appellant believes it is not) the Examiner has still failed to provide a teaching of or motivation for using successful log-in at the second and third Internet sites allowing authentication of the user at the first site. The Examiner may not simply ignore Appellant's functional limitations in the Examination process.

The portions of Hunt, relied upon by the Examiner to teach authenticating a user at a first site by sending an authentication request to a first site, causing automatic navigation to the second and third sites and attempts a login on behalf of the user with the username-password pair, successful login at the second and third sites allowing authentication of the user at the first Internet site, are provided below:

Referring to FIG. 2, in summary, the service that the interface of the registration agent site 10 provides is one of assisting internet users to complete registration forms for websites by proxy, and logging into their sites on repeat visits (Col. 4, lines 1-5).

In summary, the service that the interface of the registration agent site provides is one of assisting internet users to complete registration forms for websites by proxy, and logging into their sites on repeat visits (col. 4, lines 23-26).

Appellant points out that in Appellant's invention, the user does not wish to log-in to the second and third sites, as espoused by the Examiner when providing motivation reasoning; the server automatically navigates to these sites and logs in as the user, wherein if the user's name & password pair are successful at log-in at these two sites, **then the user is verified at the first site**, therefore, it would not be obvious because the Examiner is missing a key piece not taught in the art, which is verification at the first site depending upon successful verification of the same user at the other two sites. In the art of Hunt, a user name and password is provided at a Web site and authentication occurs *at that site*, there is no teaching or suggestion of authentication occurring at a first site as a result of successful login at a second and third site.

The Examiner's reasoning for motivation is weak, at best. The Examiner, using the exclusive art of Hunt, could not come up with any reasonable motivation for Appellant's claimed fraud prevention system without using hindsight knowledge of Appellant's invention, which is not proper examination procedure.

Examiner's arguments against dependent claims 31-33

Regarding claim 31, the system of claim 29, wherein the verification server is a first server, and the request is sent from the appliance to a second server on the network, which forwards at least a portion of the request to the first server, and the first server returns an indication of verification after causing the navigation and log-in attempt to the second and third sites provided by the user (Hunt: col. 2, lines 36-60; first server is target web server; second server is registration agent server; col. 8, lines 39-42).

Regarding claim 32, the system of claim 29, wherein all or a portion of the request is compared against stored user profile data for verification purposes (Hunt: col.3, lines 31-40; col. 2, lines 47-51).

Regarding claim 33, the system of claim 29, wherein the request comprises at least three or more user specified network destination sites and username-password pairs for the sites, and authentication is a number based on log-in results (Hunt: col. 6, lines 48-52; col. 8, lines 43- col. 9, line 15; Fig. 1).

Appellant's response

As argued above, Hunt fails to teach an authentication request at a first site, as taught and claimed in Appellant's invention. Therefore, a portion of said request cannot be compared, nor could authentication at the first site be based on log-in results at other sites. Hunt fails to teach authentication at a first site based on log-in success at other sites.

7.2 35 U.S.C. 35 U.S.C. 103(a) against claim 34

Examiner's arguments

Regarding claim 34, the Hunt reference teaches

a method for fraud prevention by authenticating a user at a first Internet site (Hunt: col. 2, lines 47-51 shows a user is verified; col. 4, lines 11-22, 30-41 teach protecting data for preventing fraud), comprising the steps of:

(a) accepting by a server an authentication request from the user comprising at least a plurality of Internet sites known to the user as capable of accepting the user's username-pair for each site and the username-password pairs are included in the authentication request from the user (Hunt: col. 2, lines 47-60; col. 6, lines 48-52);

(b) causing, by the server, automatic navigation to the sites and an automatic login attempt on behalf of the user with the username-password pairs (Hunt: col. 4, lines 1-5, 23-26); and

(c) reporting an indication of authenticity of the user according to success or failure of the login attempts (Hunt: col. 8, lines 39-42).

The Hunt reference does not explicitly state a second and third Internet site. However, the Hunt reference does address the plurality of Internet sites that a user registers and authenticates with as a problem in which the invention is overcoming (Hunt: col. 1, lines 2 1-23, 30-3 5) in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

It would have been obvious at the time of the invention to one of ordinary skill in the art to create the system of fraud preventing by Hunt to include a second and third site that a client wishes to login as taught in the background of Hunt in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

Appellant's response

Appellant points out independent method claim 34 includes similar limitations successfully argued by Appellant on behalf of claim 29, above. Therefore, claim 34 is also patentable over the art of Hunt. Appellant also points out that steps as provided in a method claim must be examined, and the art applied in the same order that the steps are provided. Clearly the Examiner has not considered the order in which the claims are presented. Additionally, step c) recites reporting an indication of authenticity of the user. Appellant points out that this stated authenticity is for the first Internet site, which is clearly ignored by the Examiner.

Depended claims 36-38 are patentable on their own merits, as argued above on behalf of claims 31-33, or at least as depended upon a patentable claim.

Summary

Appellant strongly believes that all of the claims standing are clearly and unarguably patentable over the art presented by the Examiner. Accordingly, appellant respectfully requests that the Board reverse the rejection of the claims and hold the claims allowable.

8. Claims Appendix

The claims involved in the appeal are:

1-28. (Canceled)

29. (Previously presented) A system for fraud prevention by authenticating a user at a first Internet site, comprising:

an Internet-connected verification server for performing the authentication; and
an Internet-connected appliance operable by the user for sending a request for authentication to the first Internet site;

wherein the user specifies a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user, and the server, in response to the request, causes automatic navigation to the second and third sites and attempts a login on behalf of the user with the username-password pair, successful login at the second and third sites allowing authentication of the user at the first Internet site.

30. (Canceled)

31. (Previously presented) The system of claim 29 wherein the verification server is a first server, and the request is sent from the appliance to a second server on the Internet which forwards at least a portion of the request to the first server, and the first server returns an indication of verification after causing the navigation and log-in attempt to the second and third sites provided by the user.

32. (Previously presented) The system of claim 29 wherein all or a portion of the request is compared against stored user profile data for verification purposes.

33. (Previously presented) The system of claim 29 wherein the request comprises at least three or more user specified network destination sites and user-name-password pairs for the sites, and authentication is a number based on log-in results.

34. (Previously presented) A method for fraud prevention by authenticating a user at a first Internet site, comprising steps of:

- (a) accepting by a server an authentication request from the user comprising at least a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair for each site and the username-password pairs are included in the authentication request from the user;

- (b) causing, by the server, automatic navigation to the second and third sites and an automatic login attempt on behalf of the user with the username-password pairs; and

- (c) reporting an indication of authenticity of the user according to success or failure of the login attempts.

35. (Canceled)

36. (Previously presented) The method of claim 34 wherein the server is a first server, and the request is sent from the appliance to a second server on the network, which forwards at least a portion of the request to the first server, and the first server returns the indication of authenticity after causing the navigation and log-in attempt at the sites provided by the user.

37. (Previously presented) The method of claim 34 wherein all or a portion of the request is compared against stored user profile data for verification purposes.

38. (Previously presented) The method of claim 34 wherein the request comprises three or more user specified Internet sites and username-password pairs for the sites, and authentication is a number based on log-in results.

9. Evidence Appendix

No evidence other than the arguments and facts presented in this brief is provided.

10. Related Proceedings Appendix

The present Appeal is the first Appeal submitted to the Board.

Respectfully Submitted,
Blake Earl Hayward

By /Donald R. Boys/
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
831-768-1755